

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF GEORGIA
SAVANNAH DIVISION**

UNITED STATES OF AMERICA	)	
	)	
v.	)	CR 117-34
	)	
REALITY LEIGH WINNER,	)	
	)	
Defendant.	)	

GOVERNMENT’S NOTICE OF EXPERT WITNESS TESTIMONY

Now comes the United States of America, by and through Bobby L. Christine, United States Attorney for the Southern District of Georgia, and shows as follows:

Pursuant to Federal Rule of Criminal Procedure 16(a)(1)(G), Federal Rules of Evidence 702, 703, and 705, and this Court’s Order dated March 15, 2018 (Fifth Amended Scheduling Order, doc. 240), the government provides notice to the defense of the following expert witness expected to testify at the trial of the above-referenced case. The following is a summary of the testimony this witness will provide and does not set forth every detail of his expected testimony.

A. SA David Freyman, FBI: Computer Forensic Examination¹

David Freyman is a Special Agent and Senior Forensic Examiner with the Federal Bureau of Investigation (FBI) Computer Analysis and Response Team (CART). His curriculum vitae has been provided to the defense under separate cover.² The Government expects SA Freyman will testify at trial about his examinations of the Defendant’s personal media storage

¹ “Computer forensic examination” is used in this notice to refer to the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events.

² See USAO-57755-57758.

devices, which the FBI seized from her residence on June 3, 2017. In particular, SA Freyman will discuss his examinations of the following items:

Item	FBI CART Item Number
ASUS Model 512AN-MMW	1B14
ASUS Laptop Model X553M	1B8
Amazon Tablet #PW98VM	1B13
Samsung SMG 900A Serial R88F60H6MSF	1B12
Samsung SMG 900A Serial R38F4169JAV* *This serial number was misattributed to this item on previous discovery logs, but is correct in the FBI 302 (USAO-8069).	1B9
Samsung SM-G900T	1B11

SA Freyman will explain how the FBI “imaged” each media storage device to create a digital copy of its contents. He will also explain how the FBI applied industry-standard software tools, such as Forensic Tool Kit (FTK), Internet Evidence Finder (IEF) and Cellebrite, to the forensic images to identify and collect data, such as: device and user information, documents, images, emails, text messages, internet history, bookmarks, and online messaging. The Government provided the results of these software applications to the defense on or about November 22, 2017 on a disk marked “USAO-10638.” SA Freyman also utilized industry-standard X-Ways software and virtual machine technology to examine the Defendant’s media storage devices.

SA Freyman will testify about the data described in the forensic software reports and the data found in the forensic images. For example, SA Freyman will describe the nature and appearance of websites the Defendant visited, as well as the search terms that brought her to

those sites. The testimony will be based on SA Freyman's examinations, his online research, and upon information obtained from the Internet Archive, otherwise known as the "Wayback Machine."³

SA Freyman will also explain how he conducted hands-on examinations of the Defendant's devices to find data not captured by standard forensic software. For instance, SA Freyman examined the System Resource Usage Monitor (SRUM) on the Defendant's laptop computer. SRUM monitors desktop application programs, services, windows applications and network connections. He also utilized and examined files stored within the Volume Shadow Copy Service on the Defendant's laptop computer, which is a technology that allows taking manual or automatic backup copies or snapshots of computer files or volumes, even when they are in use. SA Freyman examined the devices' registry settings, user assist directories and prefetch directories, where applicable, and examined stored files throughout the Defendant's devices.

SA Freyman will describe the operating systems of the Defendant's devices, including how the systems automatically date/time-stamp files upon the file's creation and modification. He will testify about programs downloaded, installed, and utilized on the Defendant's computer, such as the Tor Browser. SA Freyman will explain the purpose and function of the Tor Browser⁴ and of a service called SecureDrop,⁵ which is a Tor hidden service used by media outlets and their sources to anonymously share information.⁶

³ See USAO-08630-08635 and DOJ-CLASS01212-DOJ-CLASS01253. The Government is producing DOJ-CLASS01212-DOJ-CLASS01253 to the defense in classified discovery via the CISO on the date of this filing.

⁴ See www.torproject.org.

⁵ See <https://docs.securedrop.org/en/stable/source.html>;
<https://docs.securedrop.org/en/release-0.6/>.

⁶ See <https://securedrop.org/directory>.

SA Freyman will testify that he found indicia of download, installation, and usage of the Tor Browser on the Defendant's laptop computer. The usage included both uploading and downloading data. SA Freyman found a typewritten URL ending in ".onion" on the desktop of the Defendant's laptop computer. The URL corresponds to the Tor-based SecureDrop address of the news media outlet referenced in the Superseding Indictment. SA Freyman will testify that because SecureDrop is a Tor hidden service, one would expect to find little or no direct evidence of its use on a computer (other than typewritten notes saved on a desktop or other user-generated notations). In SA Freyman's opinion, the handwritten notes found in the Defendant's residence on June 3, 2017 (USAO-1098), are consistent with instructions for downloading the Tor Browser and configuring its settings for maximum anonymity. SecureDrop recommends that users employ these security settings when using its service.

SA Freyman also found an address and password for a VFEmail⁷ account on the Defendant's desktop. VFEmail, as a paid service, can provide a user with identity masking, alias accounts, and virtual forwarding boxes that rewrite the sender's metadata to hide her identity and location. Because SA Freyman located no evidence of the Defendant's use of VFEmail within her laptop computer or cellular phones, SA Freyman will opine that the Defendant could have conducted any usage of VFEmail on her devices via the Tor Browser.

In addition to VFEmail, SA Freyman will describe Slipperry.email and the service it provides. Slipperry.email is a website through which one may register for a short-term, read-only e-mail inbox – also known by Slipperry.email as a "burner" inbox. This service provides a user with a unique, disposable e-mail address, such as "Hsdjn@slipry.net." The user must provide this e-mail address to a sender, and then can only access the inbox by remembering (or

⁷ See <https://www.vfemail.net/>.

bookmarking) the unique URL, which for “Hsdxj@slipry.net” is “https://slippery.email/inbox/hsdxj/EG5icywft2o6CuNh.” The user can receive, but not send, e-mail using this address. The inbox expires and becomes inaccessible to the user after eight days. In SA Freyman’s opinion, the handwritten notes found in the Defendant’s residence on June 3, 2017 (USAO-1095), are consistent with a unique URL corresponding to a Slipry.net read-only “burner” inbox.

SA Freyman will explain the nature of “Anonymous” (a decentralized international “hactivist” group) and “WikiLeaks” (an international organization that claims to publish secret information, news leaks, and classified media) and the Defendant’s searches for and viewing of their online postings.

SA Freyman will testify about Cleanmgr.exe, which is a computer maintenance utility included in Microsoft Windows. The utility can be used to delete files such as thumbnails, downloaded program files, and temporary internet files. Based upon his examination of the laptop computer’s registry settings, and his testing of Cleanmgr.exe in a virtual environment, SA Freyman will opine that the Defendant manually initiated Cleanmgr.exe on or about April 6, 2017.

SA Freyman will testify that he compared Google search warrant results with the data found on the Defendant’s personal devices. Portions of the Defendant’s internet search and browsing history were not found in the data on her personal devices. Therefore, in SA Freyman’s opinion, the Defendant either deleted that information or used a computer other than those recovered from her residence or workspace.

SA Freyman will testify about his attribution of computer and cell phone usage to the Defendant, based upon user accounts, passwords, patterns of activity, and the following

additional discovery previously provided to the defense:

Bates Stamp	Item
USAO-002987- USAO-005872	Facebook – subscriber and transactional information
USAO-005873- USAO-007944	AT&T – subscriber and transactional information
USAO-007945- USAO-007953	Google – subscriber and transactional information
USAO-26913- USAO-26920; USAO-08636- USAO-08638	Twitter – subscriber and transactional information
USAO-10639 - USAO-10759; USAO-10828 - USAO-26725	Google – search warrant results

Based upon his examination of the information above, SA Freyman will opine that the Defendant was searching for ways to submit information anonymously to media outlets. He will also testify that the Defendant was exploring ways of transmitting information that would leave few or no forensic artifacts on her devices.

B. Memorandum of Law and Citations to Authority

The Federal Rules of Evidence provide for the admission of expert testimony when “scientific, technical, or other specialized knowledge will assist the trier of fact.” Fed. R. Evid. 702. Pursuant to Rule 702, a witness, “qualified as an expert by knowledge, skill, experience, training, or education may testify . . . in the form of an opinion or otherwise.” *Id.*

Expert testimony is admissible if it is both relevant and reliable, *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993)⁸, and where it is “the kind that enlightens and

⁸ In *Kumho Tire Co., Ltd. v. Carmichael*, 526 U.S. 137 (1999), the Supreme Court confirmed that *Daubert*’s gatekeeping obligation extends to beyond scientific experts to all of the expert matters described in Rule 702. *Kumho Tire*, 526 U.S. 149; *United States v. Paul*, 175 F.3d 906, 910 (11th Cir. 1999) (holding that the trial judge is required to inquire into the areas of

informs lay persons without expertise in a specialized field.” *United States v. Burchfield*, 719 F.2d 356, 357-58 (11th Cir. 1983). To ensure these elements are present, the trial judge serves as a “gatekeeper.” *United States v. Majors*, 196 F.3d 1206, 1215 (11th Cir. 1999) (citing *Daubert*, 509 U.S. at 2796-97). “[F]ederal district courts . . . perform [this] important gatekeeping function by screening the reliability of all expert testimony, but they have substantial discretion in deciding how to test an expert’s reliability and whether the expert’s relevant testimony is reliable.” *Majors*, 196 F.3d at 1215 (quoting *Forklifts of St. Louis, Inc. v. Komatsu Forklift, USA, Inc.*, 178 F.3d 1030, 1034 (8th Cir.1999); citing *Kumho Tire*, 119 S.Ct. at 1174-76).⁹

CONCLUSION

WHEREFORE, the government requests that the Court permit SA David Freyman, FBI, to testify as an expert in Computer Forensic Examination, pursuant to Federal Rule of Evidence 702. The proposed testimony, as detailed above, is relevant and reliable and will inform lay persons without expertise in the specialized field. Such testimony should be admitted subject to the government laying the proper evidentiary foundation at trial. Furthermore, the Government reserves the right to question the expert regarding other matters that may be raised during cross-examination by the Defendant, or based upon the testimony elicited from the defendant’s experts, if any, or other witnesses, or regarding any other evidence introduced by the Defendant. To the extent the Court allows the Defendant the same right, the government reserves the right to elicit

relevance and reliability whether the expert testimony is “scientific” or otherwise)).

⁹ A district court’s decision to admit or exclude expert testimony under Rule 702 is reviewed for abuse of discretion. *General Elec. Co. v. Joiner*, 522 U.S. 136 (1997); *United States v. Gilliard*, 133 F.3d 809, 812 (11th Cir.1998).

any additional testimony that this expert is qualified to provide should the need arise based on further developments in preparing for and during the trial.

Respectfully submitted,
BOBBY L. CHRISTINE
UNITED STATES ATTORNEY

//s// Jennifer G. Solari
Jennifer G. Solari
Assistant United States Attorney

//s// David C. Aaron

David C. Aaron
Trial Attorney
U. S. Department of Justice
National Security Division

//s// Julie A. Edelstein

Julie A. Edelstein
Deputy Chief for Counterintelligence
U. S. Department of Justice
National Security Division

//s// Amy E. Larson

Amy E. Larson
Trial Attorney
U. S. Department of Justice
National Security Division

CERTIFICATE OF SERVICE

This is to certify that I have on this day served all the parties in this case in accordance with the notice of electronic filing (“NEF”) which was generated as a result of electronic filing in this Court.

This 30th day of April 2018.

Respectfully submitted,

BOBBY L. CHRISTINE
UNITED STATES ATTORNEY

s// Jennifer G. Solari

Jennifer G. Solari
Assistant United States Attorney

Post Office Box 8970
Savannah, Georgia 31412
(912) 652-4422